A Forrester Total Economic Impact™
Study Commissioned By Barkly
May 2018

The Total Economic Impact™ Of The Barkly Endpoint Protection Platform

Cost Savings And Business Benefits Enabled By Barkly

FORRESTER®

Table Of Contents

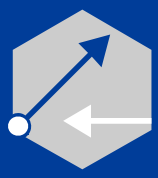
Project Director:
Kathleen Byrne

ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. Ranging in scope from a short strategy session to custom projects, Forrester's Consulting services connect you directly with research analysts who apply expert insight to your specific business challenges. For more information, visit forrester.com/consulting.

FORRESTER®

Benefits, ROI, And Payback



ROI
602%

Cost savings from avoided incidents:
$336,000

Payback:
Less than 3 months

Executive Summary

Cyberthreats are growing in frequency and complexity. Over 50% of organizations in the Forrester Data Global Business Technographics® Security Survey, 2016 had their data compromised or breached in the previous 12 months.[1] Hundreds of thousands of malware samples are uploaded every day.[2] Incidences of fileless threats are on the rise, comprising 77% of recent attacks.[3] Employee workstations are a common point of entry for attackers: A 2017 Forrester survey showed employee and corporate-owned devices as the second and third most common targets for external attacks.[4] Traditional antimalware software, which looks for known signatures, is not designed to catch these new and more complex threats, making midmarket companies that rely solely on antimalware particularly vulnerable.[5] Security professionals are looking for solutions that stop unknown threats without draining resources.

Barkly provides endpoint protection that helps its customers block today's ever-growing list of fileless attack techniques. Designed for small teams, its continuous machine learning engine ensures it stays ahead of evolving threats. Barkly commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) companies may realize by deploying the Barkly Endpoint Protection Platform. The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of the Barkly Endpoint Protection Platform on their organizations.

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed one customer that has been using Barkly for a year and a half. The customer added Barkly to its security stack, deploying it alongside its legacy antivirus (AV).

Key Findings

Quantified benefit. The interviewed organization experienced the following risk-adjusted present value (PV) quantified benefits:

- **Protection from unknown and fileless attacks prevented three incidents per year, avoiding remediation costs and lost productivity.** After installing and deploying Barkly on 600 machines just a year and a half ago, the customer has already stopped five malicious attacks. Had these attacks made it through the frontline and become incidents, the customer would have incurred expenses over $50,000 per incident in lost productivity and recovery time. Over three years, with a conservative estimate of three avoided incidents per year, the customer saves over $300,000.

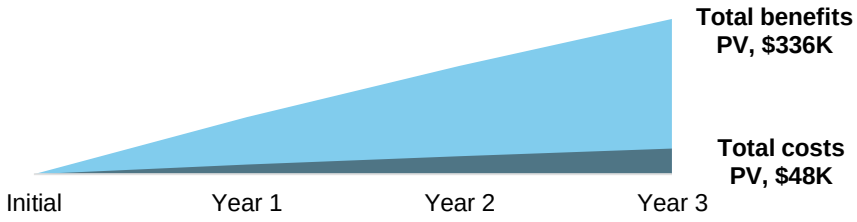
Costs. The interviewed organization experienced the following risk-adjusted PV costs:

- **Technology licensing fees.** The customer licenses Barkly for 600 machines at a cost of $18,000 per year.
- **Installation, deployment, and ongoing management.** According to the interviewee, installation and deployment "took under a minute," and ongoing management requires 1% to 2% of an admin's time.

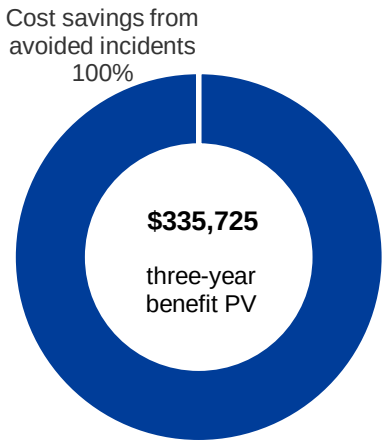
Forrester's interview with an existing customer and subsequent financial analysis found that the interviewed organization experienced benefits of $335,725 over three years versus costs of $47,858, adding up to a net present value (NPV) of $287,867 and an ROI of 602%.

FORRESTER®

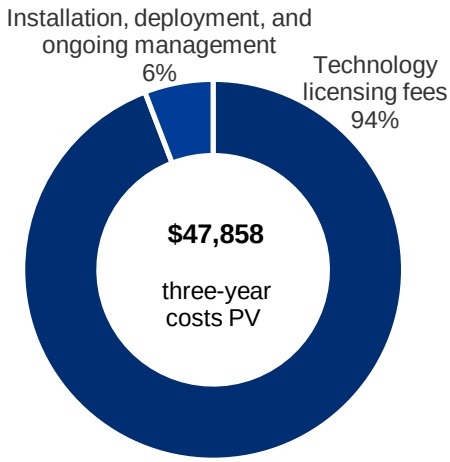
Financial Summary



Benefits



Costs



FORRESTER®

TEI Framework And Methodology

From the information provided in the interview, Forrester has constructed a Total Economic Impact™ (TEI) framework for those organizations considering implementing the Barkly Endpoint Protection Platform.

The objective of the framework is to identify the cost, benefit, flexibility, and risk factors that affect the investment decision. Forrester took a multistep approach to evaluate the impact that the Barkly Endpoint Protection Platform can have on an organization:

The TEI methodology helps companies demonstrate, justify, and realize the tangible value of IT initiatives to both senior management and other key business stakeholders.

DUE DILIGENCE
Interviewed Barkly stakeholders and Forrester analysts to gather data relative to the Barkly Endpoint Protection Platform.

CUSTOMER INTERVIEW
Interviewed one organization using the Barkly Endpoint Protection Platform to obtain data with respect to costs, benefits, and risks.

FINANCIAL MODEL FRAMEWORK
Constructed a financial model representative of the interview using the TEI methodology and risk-adjusted the financial model based on issues and concerns of the interviewed organization.

CASE STUDY
Employed four fundamental elements of TEI in modeling the Barkly Endpoint Protection Platform's impact: benefits, costs, flexibility, and risks. Given the increasing sophistication that enterprises have regarding ROI analyses related to IT investments, Forrester's TEI methodology serves to provide a complete picture of the total economic impact of purchase decisions. Please see Appendix A for additional information on the TEI methodology.

DISCLOSURES

Readers should be aware of the following:

This study is commissioned by Barkly and delivered by Forrester Consulting. It is not meant to be used as a competitive analysis.

Forrester makes no assumptions as to the potential ROI that other organizations will receive. Forrester strongly advises that readers use their own estimates within the framework provided in the report to determine the appropriateness of an investment in the Barkly Endpoint Protection Platform.

Barkly reviewed and provided feedback to Forrester, but Forrester maintains editorial control over the study and its findings and does not accept changes to the study that contradict Forrester's findings or obscure the meaning of the study.

Barkly provided the customer name for the interview but did not participate in the interviews.

The Barkly Endpoint Protection Platform Customer Journey

BEFORE AND AFTER THE BARKLY ENDPOINT PROTECTION PLATFORM INVESTMENT

Interviewed Organization

Forrester interviewed the VP of technology at an organization that uses the Barkly Endpoint Protection Platform. That customer:

- Is a $5 billion division within a global telecommunication conglomerate.
- Employs 4,000 people, 600 of whom have had Barkly running on their workstations for the past 18 months.
- Leverages a multilayered approach to endpoint protection, running Barkly alongside its legacy AV software and a multilayer defense at the network and firewall, as well as an insider threat program.

Background

The VP of technology is charged with protecting his division from ongoing security threats. As attackers become more advanced, and fileless attacks grow in frequency, he describes this task as a "constant battle." He is always on alert for a way to increase his threat protection.

Prior to deploying Barkly, he leveraged a wide array of tools to protect against attacks at the endpoint. He described Barkly as having "a unique approach that [he] felt could bear fruit in terms of impacting and stopping attacks before they become incidents." After evaluating Barkly and selecting it for its ability to stop evolving threats based on behaviors rather than signatures, he chose to add it to his endpoint protection array, running alongside his existing solutions.

> "When you look at the adversaries — whether it's criminal activity or nation-state activists — the threat is constantly evolving and changing."
>
> *VP of technology, telecommunications*

Key Results

Barkly delivered threat protection from fileless attacks without adding overhead management costs. The VP of technology at this telecommunications company expanded on this outcome:

- **Multivector, behavior-based attack blocking protects against unknown threats.** Unlike the other solutions in place at the interviewed organization, which target known signatures, Barkly monitors for suspicious behaviors and leverages machine learning to stay ahead of evolving threats. Rather than catching only known threats, "it actually stops new attacks before they happen," according to the VP of technology.
- **A lightweight solution drives full adoption among end users.** The Barkly Endpoint Protection Platform does not constantly scan files in the background. Because it's not draining resources on the machines, end users don't turn it off — which ensures that layer of protection is always in place and is an indicator that the solution is not a burden to the end user experience.

> "AV catches what's known out there, but it doesn't find anything that's new and not yet identified. Barkly was doing something I didn't see anyone else doing that at the endpoint."
>
> *VP of technology, telecommunications*

FORRESTER®

- **Straightforward installation and deployment ensures fast time-to-value.** Installation and deployment "took minutes." With a click of a button, the interviewed organization pushed the software to all 600 machines. There was no waiting for an overnight push, nor training or change management required for IT admins or end users. Instead, the solution was in place and delivering value quickly.
- **Thoughtful design points minimize incremental overhead.** The solution was designed to be managed by someone without advanced security skills: It has a clean user interface that doesn't require training to operate. Because security staff are in such high demand (and low supply) these days, reducing overhead is critical. Features like one-click-override minimize the time required to keep the software and end users operational. The interviewee described it as "low touch, high impact."

Analysis Of Benefits

QUANTIFIED BENEFIT DATA

Total Benefits

REF.	BENEFIT	YEAR 1	YEAR 2	YEAR 3	TOTAL	PRESENT VALUE
Atr	Cost savings from avoided incidents	$135,000	$135,000	$135,000	$405,000	$335,725
	Total benefits (risk-adjusted)	$135,000	$135,000	$135,000	$405,000	$335,725

The table above shows the total of all benefits across the areas listed below, as well as present values (PVs) discounted at 10%. Over three years, the interviewed organization expects risk-adjusted total benefits to be a PV of nearly $336,000.

Cost Savings From Avoided Incidents

In its first 18 months as the frontline protection on the interviewed organization's workstation, the Barkly Endpoint Protection Platform has stopped five fileless attacks, including trojan malware, power shell scripts, and malicious macros. Had these attacks been successful, the interviewed organization would have incurred costs in lost employee productivity, downtime, and remediation. The interviewee estimated an average of $50,000 in costs per incident.

For the model, Forrester assumes that Barkly prevents three incidents per year at an average cost of $50,000. That $50,000 recovery fee includes only productivity loss, business loss, and remediation costs. Readers should consider additional costs such as legal fees, the recovery of stolen data, and reputation damage.

This benefit will vary based on:

- The number of endpoints in use.
- The actual cost of a breach, which is impacted by:
  - The severity of the incident.
  - The cost of lost business and lost productivity.

To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year risk-adjusted total PV of $335,725.

In its first 18 months, Barkly has detected and blocked five fileless attacks.

Impact risk is the risk that the business or technology needs of the organization may not be met by the investment, resulting in lower overall total benefits. The greater the uncertainty, the wider the potential range of outcomes for benefit estimates.

Costing Savings From Avoided Incidents: Calculation Table

REF.	METRIC	CALC.	YEAR 1	YEAR 2	YEAR 3
A1	Cost to recover from an incident		$50,000	$50,000	$50,000
A2	Annual incidents avoided		3	3	3
At	Cost savings from avoided incidents	A1*A2	$150,000	$150,000	$150,000
	Risk adjustment	↓10%			
Atr	Cost savings from avoided incidents (risk-adjusted)		$135,000	$135,000	$135,000

Flexibility

The value of flexibility is clearly unique to each customer, and the measure of its value varies from organization to organization. There are multiple scenarios in which a customer might choose to implement the Barkly Endpoint Protection Platform and later realize additional uses and business opportunities, including:

- **Cost savings from retiring antivirus software.** The interviewee envisions a scenario in which he can eliminate his AV software and solely run Barkly on his workstations, eliminating associated technology fees.
- **Deploying on additional workstations and servers.** The interviewed organization can deploy Barkly on additional servers or workstations, increasing its protection and, ultimately, benefits.

Flexibility would also be quantified when evaluated as part of a specific project (described in more detail in Appendix A).

Flexibility, as defined by TEI, represents an investment in additional capacity or capability that could be turned into business benefit for a future additional investment. This provides an organization with the "right" or the ability to engage in future initiatives but not the obligation to do so.

Analysis Of Costs

QUANTIFIED COST DATA

Total Costs

REF.	COST	INITIAL	YEAR 1	YEAR 2	YEAR 3	TOTAL	PRESENT VALUE
Btr	Technology licensing fees	$0	$18,000	$18,000	$18,000	$54,000	$44,763
Ctr	Installation, deployment, and ongoing management	$254	$1,142	$1,142	$1,142	$3,681	$3,095
	Total costs (risk-adjusted)	$254	$19,142	$19,142	$19,142	$57,681	$47,858

Technology Licensing Fees

Fees to Barkly are based on the number of endpoints and include both licensing and support. The organization installed Barkly on 600 workstations at $18,000 per year.

An organization's licensing fees will vary based on the number of endpoints. Barkly provided realistic fees, so the cost is not risk-adjusted, yielding a three-year risk-adjusted total PV of $44,763.

The table above shows the total of all costs across the areas listed below, as well as present values (PVs) discounted at 10%. Over three years, the interviewed organization expects risk-adjusted total costs to be a PV of nearly $48,000

Technology Licensing Fees: Calculation Table

REF.	METRIC	CALC.	YEAR 1	YEAR 2	YEAR 3
B1	Technology licensing fees		$18,000	$18,000	$18,000
	Risk adjustment	0%			
Btr	Technology licensing fees (risk-adjusted)		$18,000	$18,000	$18,000

Installation, Deployment, And Ongoing Management

The interviewee described installation as requiring just "one stroke of a button" to deploy to 600 machines. Because of its intuitive interface and lightweight agent, it took one admin just minutes to complete. With a zero-failure rate and no conflicts with other software, there was no rework or follow-up required. End users did not have to upgrade their machines, so no employee communication campaign was required. To be conservative, the model assumes 4 hours of an admin's time.

Ongoing management of the solution is minimal, with an estimated 1.5 hours of an admin's time dedicated to the task each month. The admin's tasks included overriding false positives and overall threat monitoring. This admin did not require advanced security skills and easily absorbed the task into his responsibilities.

These costs will vary based on:

- Any customizations required.
- Number of users.

Installation, deployment, and ongoing management required less than 18 hours per year.

FORRESTER®

› Average fully loaded salaries.

To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year risk-adjusted total PV of $3,095.

Implementation risk is the risk that a proposed investment may deviate from the original or expected requirements, resulting in higher costs than anticipated. The greater the uncertainty, the wider the potential range of outcomes for cost estimates.

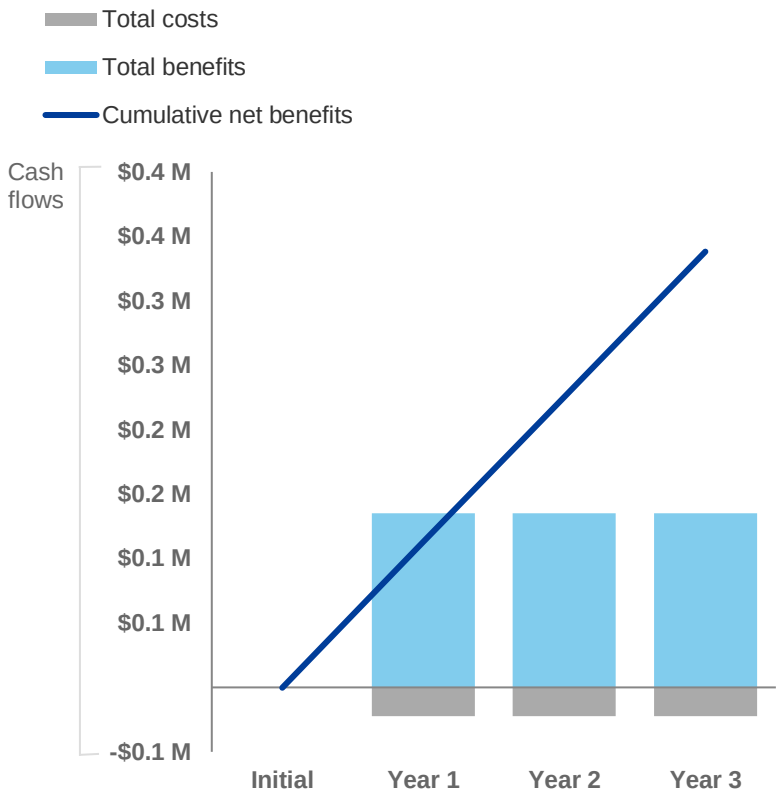
Installation, Deployment, And Ongoing Management: Calculation Table

REF.	METRIC	CALC.	INITIAL	YEAR 1	YEAR 2	YEAR 3
C1	Hours required for installation and deployment (one time)		4	0	0	0
C2	Hours required for ongoing management (monthly)			1.5	1.5	1.5
C3	Annual salary for IT admin		$120,000	$120,000	$120,000	$120,000
C4	Resource costs for installation and deployment	=C1*C3/2,080	$231			
C5	Resource costs for ongoing management	=C2*C3/2,080*12		$1,038	$1,038	$1,038
Ct	Installation, deployment, and ongoing management	=C4+C5	$231	$1,038	$1,038	$1,038
	Risk adjustment	↑10%				
Ctr	Installation, deployment, and ongoing management (risk-adjusted)		$254	$1,142	$1,142	$1,142

Financial Summary

CONSOLIDATED THREE-YEAR RISK-ADJUSTED METRICS

Cash Flow Chart (Risk-Adjusted)



The financial results calculated in the Benefits and Costs sections can be used to determine the ROI, NPV, and payback period for the interviewed organization's investment. Forrester assumes a yearly discount rate of 10% for this analysis.

These risk-adjusted ROI, NPV, and payback period values are determined by applying risk-adjustment factors to the unadjusted results in each Benefit and Cost section.

Cash Flow Table (Risk-Adjusted)

	INITIAL	YEAR 1	YEAR 2	YEAR 3	TOTAL	PRESENT VALUE
Total costs	($254)	($19,142)	($19,142)	($19,142)	($57,681)	($47,858)
Total benefits	$0	$135,000	$135,000	$135,000	$405,000	$335,725
Net benefits	($254)	$115,858	$115,858	$115,858	$347,319	$287,867
ROI						602%
Payback period						<3

FORRESTER®

Barkly Endpoint Protection Platform: Overview

The following information is provided by Barkly. Forrester has not validated any claims and does not endorse Barkly or its offerings.

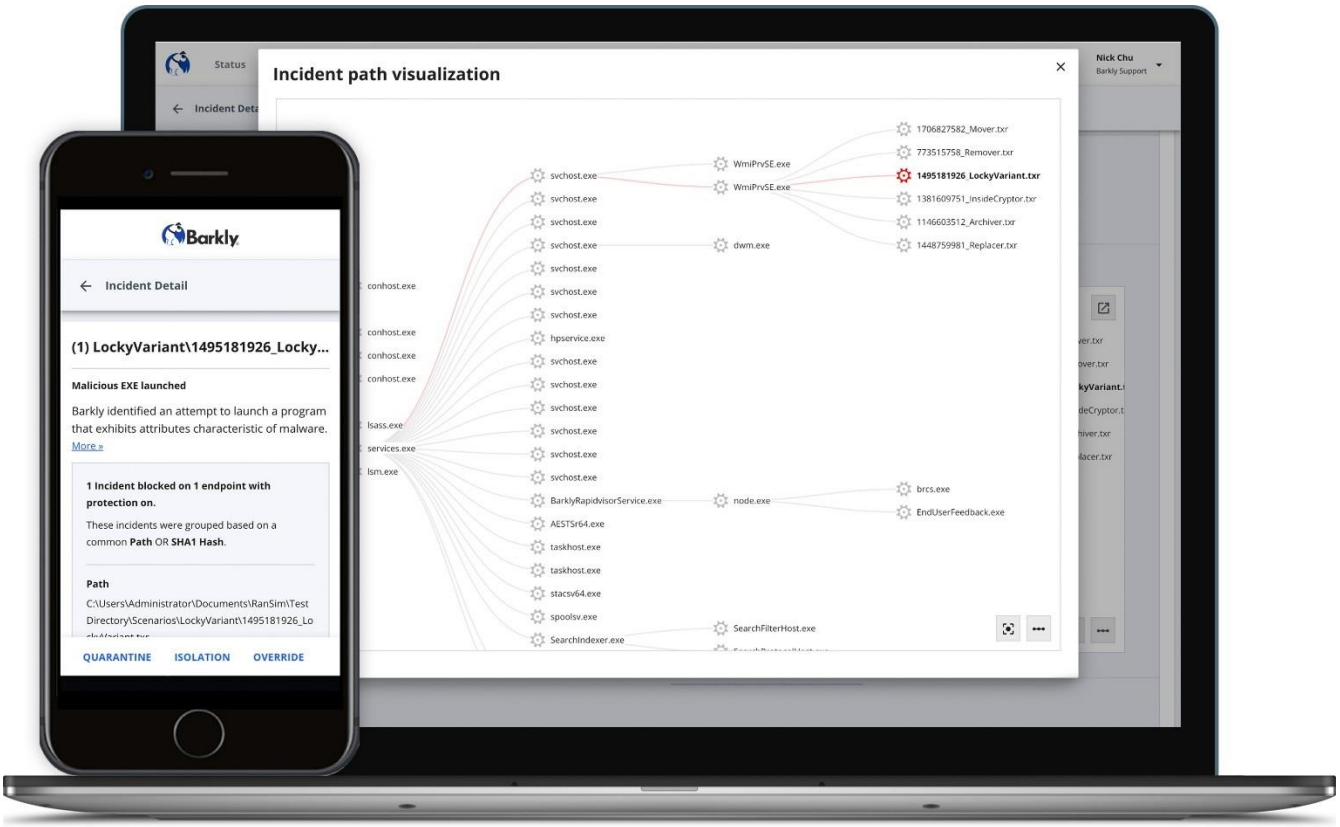
Barkly advances endpoint protection and replaces legacy antivirus with the strongest protection, the smartest technology, and the simplest management. There are three key components of the Barkly Endpoint Protection Platform™: Barkly ProtectIQ™, Barkly EvolveIQ™, and Barkly CommandIQ™.

Barkly ProtectIQ™ delivers the strongest protection against the infection and exploitation techniques used in today's complex attacks. ProtectIQ uses Barkly's patented three-level architecture and ability to combine information from native CPU-level hardware capabilities, kernel-level drivers, and user space analytics for an unmatched ability to see and block attacks in real time. ProtectIQ is delivered through the Barkly Rapidvisor® agent, which is local on the endpoint and extremely lightweight, consuming less than 1% of CPU.

Barkly EvolveIQ™ automatically converts malware intelligence into powerful protection through its Continuous Machine Learning Engine that trains models nightly against the latest malware and goodware. The result is maximized protection against new and unknown threats and minimized false positives for customers.

Barkly CommandIQ™ provides a simple, cloud-based management experience with automated incident response from any desktop or mobile device. Administrators can immediately respond to alerts and investigate attacks with one-click isolation and quarantine, root cause identification, and attack visualization. Organizations can deploy Barkly in minutes, without security expertise, policy management, or any configuration.

Barkly is independently certified for antivirus replacement, HIPAA, PCI DSS, and NIST and receives top reviews from third-party organizations and communities such as SC Magazine, Capterra, and Spiceworks. Barkly is formed by an elite team of security and software-as-a-service (SaaS) experts from IBM, Cisco, and Intel and is backed by investors NEA and Sigma Prime.



FORRESTER®

Appendix A: Total Economic Impact

Total Economic Impact is a methodology developed by Forrester Research that enhances a company's technology decision-making processes and assists vendors in communicating the value proposition of their products and services to clients. The TEI methodology helps companies demonstrate, justify, and realize the tangible value of IT initiatives to both senior management and other key business stakeholders.

Total Economic Impact Approach

Benefits represent the value delivered to the business by the product. The TEI methodology places equal weight on the measure of benefits and the measure of costs, allowing for a full examination of the effect of the technology on the entire organization.

Costs consider all expenses necessary to deliver the proposed value, or benefits, of the product. The cost category within TEI captures incremental costs over the existing environment for ongoing costs associated with the solution.

Flexibility represents the strategic value that can be obtained for some future additional investment building on top of the initial investment already made. Having the ability to capture that benefit has a PV that can be estimated.

Risks measure the uncertainty of benefit and cost estimates given: 1) the likelihood that estimates will meet original projections and 2) the likelihood that estimates will be tracked over time. TEI risk factors are based on "triangular distribution."

The initial investment column contains costs incurred at "time 0" or at the beginning of Year 1 that are not discounted. All other cash flows are discounted using the discount rate at the end of the year. PV calculations are calculated for each total cost and benefit estimate. NPV calculations in the summary tables are the sum of the initial investment and the discounted cash flows in each year. Sums and present value calculations of the Total Benefits, Total Costs, and Cash Flow tables may not exactly add up, as some rounding may occur.

Present value (PV)

The present or current value of (discounted) cost and benefit estimates given at an interest rate (the discount rate). The PV of costs and benefits feed into the total NPV of cash flows.

Net present value (NPV)

The present or current value of (discounted) future net cash flows given an interest rate (the discount rate). A positive project NPV normally indicates that the investment should be made, unless other projects have higher NPVs.

Return on investment (ROI)

A project's expected return in percentage terms. ROI is calculated by dividing net benefits (benefits less costs) by costs.

Discount rate

The interest rate used in cash flow analysis to take into account the time value of money. Organizations typically use discount rates between 8% and 16%.

Payback period

The breakeven point for an investment. This is the point in time at which net benefits (benefits minus costs) equal initial investment or cost.

Appendix B: Endnotes

[1] Source: “Forrester Data: Endpoint Security Software Forecast, 2016 To 2021 (Global),” August 22, 2017.

[2] Source: “Enterprise Risk Index: Risk assessment and control factors Q2 2017,” SentinelOne, 2017 (https://go.sentinelone.com/rs/327-MNM-087/images/SEN0202_Whitepaper_EnterpriseRiskIndex_FINAL%20%282%29.pdf).

[3] Source: “The 2017 State of Endpoint Security Risk Report,” Ponemon Institute, 2017 (https://www.barkly.com/ponemon-2018-endpoint-security-statistics-trends).

[4] Source: “The Forrester Wave™: Endpoint Security Suites, Q4 2016,” October 19, 2016.

[5] “Forrester Data: Endpoint Security Software Forecast, 2016 To 2021 (Global),” August 22, 2017.